

CLAIMS

What is claimed is:

1. A method of affecting a trustworthy-measure associated with a source node (110) in a distributed network, comprising: receiving an information file from the source node (110) and a corresponding identifying code (CSC) that is based on content of the information file when the information file is introduced to the network, computing (230) an associated code (CSC') based on received content of the information file; comparing (232) the associated code (CSC') with the identifying code (CSC); and transmitting (240) an error report to an administrator node (130), identifying the source node (110) and the information file, when at least one of the following occur: the associated code (CSC') does not correspond to the identifying code (CSC), and the content of the information file is abnormal; thereby facilitating a reduction of the trustworthy-measure associated with the source node (110).
2. The method of claim 1, further including: repeating (234) the receiving, computing, and comparing steps prior to transmitting the error report.
3. The method of claim 1, wherein the identifying code (CSC) includes at least one of: a control-sum-code, and a hash-value.
4. The method of claim 1, wherein the error report includes the associated code (CSC') and the identifying code (CSC).
5. A method of facilitating control of distribution of modified or corrupted files in a distributed network, comprising: providing a catalog of available files to nodes of the distributed network, the catalog identifying each file of the available files and a corresponding source node (110) of each file, processing (250) an error report from a target node (120) that received a downloaded file from a selected source node (110), verifying (260-285) the error report, degrading (290) a trustworthy-measure of at least one node of the distributed network based on a result of verifying the error report, and providing the trustworthy-measure of the at least one node to other nodes of the distributed network.
6. The method of claim 5, wherein the catalog includes a parameter that is based on the trustworthy-measure of each source node (110).
7. The method of claim 5, wherein the error report is based on at least one of: a modification of an original version of the downloaded file, and an abnormality associated with the downloaded file.

8. The method of claim 5, wherein verifying (260-285) the error report is based upon an identifying code (CSC) corresponding to an original version of the downloaded file.

9. The method of claim 8, wherein the catalog includes the identifying code (CSC).

10. A method of controlling a trustworthy-measure associated with a source node (110) in a distributed network, comprising: receiving (270), from a reporting node (120), a report of a modification or corruption of an information file by the source node (110), determining (260-285) a validity of the report, and degrading (290) the trustworthy-measure associated with the source node (110) when the report is determined to be valid.

11. The method of claim 10, wherein determining (260-285) the validity of the report includes: receiving (270), from the source node (110), the information file and a corresponding identifying code (CSC) that is based on content of the information file when the information file is introduced to the network, computing (280) a verification code (CSC") based on received content of the information file, comparing (285) the verification code (CSC") with the identifying code (CSC).

12. The method of claim 10, further including degrading (295) a trustworthy-measure associated with the reporting node (120) when the report is determined to be invalid.

13. The method of claim 10, further including allowing the trustworthy-measure to be accessed by other nodes in the distributed network, to influence subsequent requests for material from the source node (110), based on the trustworthy-measure.

14. The method of claim 10, wherein determining the validity of the report includes notifying (320) the source node (110) of the report, and assessing (325-350) a response from the source node (110) to determine the validity of the report.

15. The method of claim 14, wherein assessing (325-350) the response includes: determining (325-330) that the report is valid if the response is a null-response, or an admittance of effecting the modification or corruption of the information, and revising (325-340) the report to identify an alternative source of the modification or corruption of the information, if the response includes an acknowledgement of the modification or corruption.

16. The method of claim 14, wherein assessing the response includes assessing (450, 460) the reliability of at least one of: the information file, the source node (110), and the reporting node (120).

17. The method of claim 10, wherein determining the validity of the report includes determining (460) a reliability of the source node (110), and determining (460) the reliability of the source node (110) is based on at least one of: the trustworthy-measure of the source node (110), longevity of the source node (110) within the distributed network, traffic flow via the source node (110), and prior activities of the source node (110).

18. The method of claim 17, wherein determining the validity of the report also includes determining (460) a reliability of the reporting node (120), and determining (460) the reliability of the reporting node (120) is based on at least one of: the trustworthy-measure of the reporting node (120), longevity of the reporting node (120) within the distributed network, traffic flow via the reporting node (120), and prior activities of the reporting node (120).

19. The method of claim 10, wherein determining the validity of the report includes a verification (420-430) of prior ownership of the information file.

20. A communications network, comprising: a plurality nodes, including at least a source node (110), a target node (120), and an administrator node (130), the source node (110) having an information file and a corresponding identifying code (CSC) based on content of the information file at a prior point in time, the target node (120) being configured to: receive (220) the information file and identifying code (CSC), transmit (240) a discrepancy report based on at least one of: a discrepancy between the identifying code (CSC) and a computed code (CSC') based on received content of the information file, and an abnormality in the information file, and the administrator node (130) being configured to: receive (250, 310) the discrepancy report, and modify (290) a trustworthy-measure associated with at least one node of the plurality of nodes, based on the discrepancy report.

21. the communications network of claim 20, wherein the administrator node (130) is further configured to verify the discrepancy report prior to modifying the trustworthy-measure.

22. The communications network of claim 21, wherein the administrator node (130) is configured to verify the discrepancy report by: receiving (270) the information file from the source node (110), and determining (280) a verification code (CSC'') based on

received content of the information file, and comparing (285) the verification code (CSC") to the identifying code (CSC).

23. The communications network of claim 21, wherein the administrator node (130) is configured to verify the discrepancy report based on at least one of: a reliability of the received content of the information file, a record of prior ownership of the information file, a reliability of the source node (110), a reliability of the reporting node (120), a longevity of the source node (110) within the network, a longevity of the reporting node (120) within the network, prior activities of the source node (110) within the network, and prior activities of the reporting node (120) within the network.

24. The communications network of claim 23, wherein the trustworthy-measure of the source node (110) is available for access by each of the plurality of nodes, to facilitate control of subsequent distribution of files from the source node (110) based on the trustworthy-measure.

25. An administrator node (130) in a communications network comprising a plurality nodes, that is configured to: receive (250, 310) a discrepancy report from a reporting node (120), the discrepancy report identifying a source node (110) and an information file, verify (280, 350) the discrepancy report, and modify (290, 295) a trustworthy-measure associated at least one node of the plurality of nodes, based on whether the discrepancy report is valid.

26. The administrator node (130) of claim 25, wherein the discrepancy report is based on a comparison of a code (CSC') computed by the reporting node (120) to an identifying code (CSC) corresponding to contents of the information file at a prior time, the administrator node (130) is configured to verify the discrepancy report by: receiving the information file from the source node (110), and determining a verification code (CSC") based on received content of the information file, and comparing the verification code (CSC") to the identifying code (CSC).

27. The administrator node (130) of claim 25, wherein the administrator node (130) is configured to verify the discrepancy report based on at least one of: a reliability of the received content of the information file, a record of prior ownership of the information file, a reliability of the source node (110), a reliability of the reporting node (120), a longevity of the source node (110) within the network, a longevity of the reporting node (120) within the network, prior activities of the source node (110) within the network, and prior activities of the reporting node (120) within the network.

28. The administrator node (130) of claim 25, wherein the administrator node (130) is further configured to provide a catalog that identifies a plurality of information files and corresponding source nodes (110).

29. The administrator node (130) of claim 28, wherein the catalog further includes a parameter based on the trustworthy-measure of the at least one node.